



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/759,596

01/15/2004

Christopher Newell Toomey

AOL0133

8695

22862 7590 09/08/2009

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER

KHOSHNOODI, NADIA

ART UNIT

PAPER NUMBER

2437

NOTIFICATION DATE

DELIVERY MODE

09/08/2009

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eptomatters@glenn-law.com

Office Action Summary	Application No. 10/759,596	Applicant(s) TOOMEY, CHRISTOPHER NEWELL	
	Examiner NADIA KHOSHNOODI	Art Unit 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 May 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4,5,8-10,12-16,19-29,32-38,41,42,45-47,49-53,56-66 and 69-74 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,4,5,8-10,12-16,19-29,32-38,41,42,45-47,49-53,56-66 and 69-74 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 1/15/2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

Claims 2-3, 6-7, 11, 17-18, 30-31, 39-40, 43-44, 48, 54-55, 67-68, & 75-94 are cancelled. Applicant's arguments/amendments with respect to pending claims 1, 4-5, 8-10, 12-16, 19-29, 32-38, 41-42, 45-47, 49-53, 56-66, & 69-74 filed 5/15/2009 have been fully considered but are moot in view of new grounds rejection, however Examiner has addressed certain arguments below. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

Applicants repeatedly contend that the claimed invention is not directed to using an IP address as a client identifier in the remarks, however the claims themselves do not limit the scope of the invention in this manner. Specifically, there is no mention in the claims to positively recite specifically what the client identifier may be. If Applicants wish, they are more than welcome to incorporate language into the claims which specify that the client identifier is one of a MAC address, a disk serial number, or anything else supported by the specification in order to distinguish it from an IP address. However, Examiner would like to point out that even if the claims were limited in this manner, the prior art found in a search (US Pub. 2004/0034797) and cited below may still read on that limitation as well. Thus, although Applicants have attempted to overcome the prior art in a manner that would serve to remove the client-ID from being interpreted as an IP address, Examiner does not agree with this notion. Specifically, the notion of a static IP address which is always unique to a client, i.e. not a temporary client/user binding as argued, and which may be locally generated on a client, as suggested by Chiles et al.

(having a publication date of more than a year before the filing date for the present application) detailed below, serves as a client-originated item of data.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

II. Claims 1, 4-5, 8-9, 12-16, 19-28, 32-33, 35-36, 38, 41-42, 45-46, 49-53, 56-65, 70, and 72-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goertzel et al., US Patent No. 6,308,273; and further in view of Chiles et al., US 7,353,280 (having a prior publication date of Oct. 25, 2001) and Hibberd, US Patent No. 7,454,794.

As per claims 1 and 38:

Goertzel et al. substantially teach a method/computer program product on a computer readable medium, comprising the steps of: identifying entities legitimately entitled to service, wherein an entity comprises a user ID-client pair, said user id-client pair comprising an individual user-machine combination (col. 6, lines 30-35 and col. 7, lines 5-9); establishing said identified entities as trusted entities by issuing a trust token for each entity successfully authenticating to said network service, said trust token comprising a data object that includes a client identifier, said client identifier comprising at least one item of data that uniquely identifies the client machine, wherein a user ID-client pair represents a unique entity (col. 5, lines 12-58 and col. 10, lines 38-55); storing said issued trust token on said client (col. 9, lines 3-19);

transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to network service (col. 8, lines 34-43); determining whether each request is a trusted or an untrusted login (col. 7, lines 1-37); processing requests from said trusted entities according to a first policy (col. 7, lines 1-37); and processing remaining requests according to at least a second policy (col. 7, lines 1-37).

Not explicitly disclosed is wherein the client identifier comprises at least one client-originated item of data that uniquely identifies the client machine. However, Chiles et al. teach that a client machine may be configured with a local address, such as a static IP address which is then made known to a gateway device to help facilitate communications over a network (col. 14, lines 35-38; col. 15, lines 16-30 and lines 47-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Goertzel et al. to use a static IP address which originates on a client machine and is used to uniquely identify the client machine. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chiles et al. suggest that using a manually assigned static IP address results in a permanent binding which can allow a host system to recognize the individual client device that is initiating the communication in col. 14, lines 42-44.

Also, not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises adding a specified amount of incremental response latency when processing untrusted logins, wherein untrusted logins comprise successful and unsuccessful logins from entities determined to lack a trust token. However, Hibberd teaches that a client's identifier is used to verify the entity as an authorized entity and subjects the client to a rate limit

until the verification step has been successfully completed (col. 3, lines 44-53). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Goertzel et al. to process requests from clients that are not trusted should be subjected to rate limiting procedures. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Hibbard suggests that adding incremental response latency for untrusted connections from a particular client can limit the amount of damage a hacker/untrusted entity can do to a system in col. 3, lines 18-30.

As per claims 4 and 41:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 1 and 39. Furthermore, Goertzel et al. teach wherein entities legitimately entitled to service comprise entities previously able to successfully authenticate to a network service (col. 6, lines 1-12).

As per claims 5 and 42:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 4 and 41. Furthermore, Goertzel et al. teach wherein said network service comprises a server (col. 5, lines 4-11).

As per claims 8 and 45:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 1 and 38. Furthermore, Goertzel et al. teach said data object including: said user ID or a derivative thereof (col. 9, lines 5-19).

As per claims 9 and 46:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 8 and 45. Furthermore, Goertzel et al. teach wherein said derivative comprises a cryptographic hash of the user ID (col. 11, lines 54-60).

As per claims 12 and 49:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 11 and 38. Furthermore, Goertzel et al. teach said client identifier comprising any of: a client identifier assigned by said network service; and a client identifier provided by the client (col. 6, lines 1-12).

As per claims 13 and 50:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 7 and 45. Furthermore, Goertzel et al. teach further comprising a step of encrypting said trust token (col. 17, lines 6-14).

As per claims 14 and 51:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claim 13 and 50. Furthermore, Goertzel et al. teach further comprising the step of: transmitting said trust token from said network service to said client upon successful authentication to said network service by said entity (col. 16, lines 35-54).

As per claims 15 and 52:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 14 and 51. Furthermore, Goertzel et

Art Unit: 2437

al. teach wherein said step of transmitting said trust token occurs via a secure channel (col. 17, lines 6-14).

As per claims 16 and 53:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 15 and 52. Furthermore, Goertzel et al. teach wherein said secure channel comprises a network connection secured via the SSL (secure sockets layer) protocol (col. 17, lines 6-14).

As per claims 19 and 56:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 1 and 38. Furthermore, Goertzel et al. teach wherein said step of transmitting said stored, issued trust token occurs via a secured channel (col. 17, lines 6-14).

As per claims 20 and 57:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 19 and 56. Furthermore, Goertzel et al. teach wherein said secured channel comprises a network connection secured via the SSL (secure sockets layer) protocol (col. 17, lines 6-14).

As per claims 21 and 58:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 12 and 50. Furthermore, Goertzel et al. teach further comprising a step of storing said issued trust token in a server side database, indexed according to a combination of user ID and client identifier (col. 7, lines 1-15 and col. 8,

lines 34-44).

As per claims 22 and 59:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Goertzel et al. teach further comprising the step of: transmitting said client identifier assigned by said network service from said network service to said client upon successful authentication to said network service by said entity (col. 16, lines 35-54).

As per claims 23 and 60:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 22 and 59. Furthermore, Goertzel et al. teach wherein said step of transmitting said client identifier assigned by said network service occurs via a secure channel (col. 17, lines 6-14).

As per claims 24 and 61:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 22 and 59. Furthermore, Goertzel et al. teach wherein said secure channel comprising a network connection secured via the SSL (secure sockets layer) protocol (col. 17, lines 6-14).

As per claims 25 and 62:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Goertzel et al. teach the method/ computer program product on a computer readable medium further comprising the steps of: transmitting said user ID and client identifier to said server; and

retrieving said stored trust token from said database (col. 8, lines 34-62).

As per claims 26 and 63:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Goertzel et al. teach wherein said server side database serves a plurality of services (col. 8, lines 34-43).

As per claims 27 and 64:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 2 and 40. Furthermore, Goertzel et al. teach wherein processing requests from said trusted entities according to a first policy comprises the steps of: validating said trust token (col. 7, lines 1-15 and col. 9, lines 5-39); and processing request without adding incremental response latency (col. 7, lines 16-19 and col. 9, lines 39-43).

As per claims 28 and 65:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 27 and 64. Furthermore, Goertzel et al. teach wherein said step of validating said trust token comprises the step of: verifying that the user ID and a client identifier in the trust token match those presented by the client on the request (col. 9, lines 5-39).

As per claim 32:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method of claim 31. Furthermore, Hibbard teaches wherein response latency is added to a configurable percentage of successful untrusted logins (col. 4, lines 19-48).

As per claims 33 and 70:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 1 and 38. Furthermore, Hibbard teaches wherein processing remaining requests according to at least a second policy comprises adding a specified amount of incremental response latency when processing requests from untrusted IP addresses that have exceeded a configurable login rate (col. 3, lines 14-30).

As per claims 35 and 72:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 1 and 39. Furthermore, Goertzel et al. teach wherein said policies are applied by a server (col. 8, lines 34-43 and col. 10, lines 38-63).

As per claims 36 and 73:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 35 and 72. Furthermore, Hibbard teaches wherein said server applies rate policies for a plurality of network devices (col. 2, lines 39-55).

III. Claims 10, 29, 37, 47, 66, and 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goertzel et al., US Patent No., 6,308,273; Chiles et al., US 7,353,280 (having a prior publication date of Oct. 25, 2001); and Hibbard, US Patent No. 7,454,794 as applied to claims 6, 8, 28, 38, 45, and 65 above, and further in view of Pallante, US Pub. No. 2003/0028495.

As per claims 10 and 47:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 8 and 45. Not explicitly disclosed is wherein said data object further includes any of: a time stamp of first authentication to said network service by said entity; and a time stamp of a most recent authentication to said network service by said entity. However, Pallante teaches that logs are kept with timestamps of when users were authenticated in order to access documents. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Goertzel et al. to maintain a time stamp for a first and most recent authentication when the entity accesses the system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that time-stamping and maintaining a log with the time-stamping information is important in non-repudiation proofs in par 154.

As per claims 29 and 66:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 28 and 65. Not explicitly disclosed is wherein said step of validating said trust token further comprises any of the steps of: verifying that a time stamp of a first authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable first-authentication time stamp; and verifying that a time stamp of a last authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable last-authentication time stamp. However, Pallante teaches wherein the token is a certificate which holds a validity period of when the entity can gain access to the system. Therefore, it would have been obvious to a person in the art at the time the

Art Unit: 2437

invention was made to modify the method disclosed in Goertzel et al. to enhance the security of the system by using a certificate instead of a password as the trust token and to allow access based on the validity period as defined by the certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that using a certificate and abiding by the validity periods is important to ensure that entities do not gain access unless they are allowed based on their privileges in par. 99.

As per claims 37 and 74:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 6 and 38. Not explicitly disclosed is further comprising the step of: updating said trust token after a login by a trusted entity. However, Pallante teaches that the trusted token may be a certificate in order to increase security, as well as renewing certificates when appropriate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Goertzel et al. to use a certificate as the trust token and to renew it when necessary. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that renewing a certificate will further ensure that appropriate entities gain access to resources for the full duration of the amount of time they are entitled to do so in par. 51.

IV. Claims 34 and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goertzel et al., US Patent No., 6,308,273; Chiles et al., US 7,353,280 (having a prior publication

date of Oct. 25, 2001); and Hibbard, US Patent No. 7,454,794 as applied to claims 1 and 38 above, and further in view of Card, US Pub. No. 2002/0073339.

As per claims 34 and 71:

Goertzel et al., Chiles et al., and Hibbard substantially teach the method/computer program product on a computer readable medium of claims 1 and 38. Not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises requiring an untrusted entity to complete a Turing test. However, Card teaches that questioning the user based on information that only the user would know allows for stronger authentication.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Goertzel et al. to subject an untrusted entity to complete a Turing test in order to determine whether or not that user is a valid user or if the user should remain untrusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Card suggests that requiring the user to answer a security question, which is known only to that user, in order to establish whether or not he/she should be trusted allows for stronger authentication in par. 43.

V. Claim 69 is rejected under 35 U.S.C. 103(a) as being unpatentable over Goertzel et al., US Patent No., 6,308,273; Chiles et al., US 7,353,280 (having a prior publication date of Oct. 25, 2001); and Hibbard, US Patent No. 7,454,794 as applied to claim 38 above, and further in view of Malan, US Pub. No. 2002/0032793.

As per claim 69:

Goertzel et al., Chiles et al., and Hibbard substantially teach the computer program product on a computer readable medium of claim 38. Not explicitly disclosed is wherein response latency is added to a specified percentage of successful logins. However, Malan et al. teach that if malicious use of the network resources is detected based on malicious activity on a connection (regardless of whether or not the entity is trusted), that particular connection may be subjected to a cut-back on the connection rate (par. 69-70). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Goertzel et al. to add incremental response latency if an untrusted login has been detected. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Malan et al. suggest that when malicious activity is detected an important measure in preventing an attack is to contain the amount of damages that may be incurred in par. 67-68.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,510,513
2. US Pub. No. 2003/0078035 – local IP address generation
3. US Pub. No. 2004/0034797 – utilizes unique client ID (MAC address) and unique user ID pair in a method for implementing access control

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
8/27/2009

NK

/Emmanuel L. Moise/

Application/Control Number: 10/759,596
Art Unit: 2437

Page 16

Supervisory Patent Examiner, Art Unit 2437